

SPECIFICATION AMENDMENTS

As supported by the paragraph beginning at line 5, page 9, please amend the specification as follows:

Substitute the paragraph beginning at line 17, page 9, with the following:

$SIGN(M_1, M_2)$

Find a k with $H_0(M_1, g^k) = M_2$.

$r = H_1(M_1, g^k)$

$s = k/(r + 1) - x H_2(M_1, g^k) \mod q$

$auth = H_3(BK, g^k)$

return $(M_1, r, s, auth)$, which is one embodiment of the digital

signature